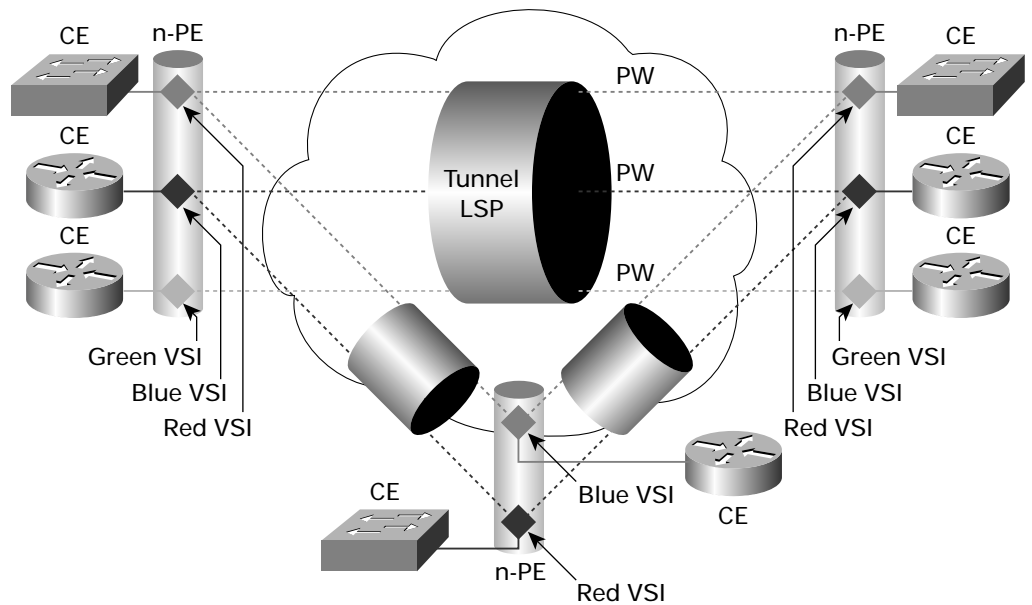


# Cisco IOS MPLS Virtual Private LAN Service

**Virtual Private LAN Service (VPLS)** is generating considerable interest with enterprises and service providers as it offers multipoint Ethernet LAN services, often referred to as transparent LAN service (TLS), over MPLS networks. In operation a VPLS offers the same connectivity experienced if a device were attached to an Ethernet switch. The IETF VPLS documents describe an architecture that links virtual switch instances (VSIs) using Multiprotocol Label Switching (MPLS) pseudowires to form an “emulated” Ethernet switch. Please refer to Figure 1 for a schematic representation of VPLS components.

Figure 1  
VPLS Components



Legend	
CE:	Customer Edge Device
n-PE:	Network-Facing Provider Edge
VSI:	Virtual Switch Instance
PW:	Pseudowire
Tunnel LSP:	Tunnel Label Switch Path That Provides PW Transport

VPLS enables service providers with MPLS networks to offer geographically dispersed Ethernet Multipoint Service (EMS), aka Ethernet Private LAN Service as defined by Metropolitan Ethernet Forum (MEF). These services are becoming attractive as many Enterprise applications, such as IP Telephony, utilize peer-to-peer operation that benefit from any-to-any connectivity, which is one of the key attributes of EMS in that each customer edge device or node communicates directly with all



other customer edge nodes associated with the EMS. By contrast, a hub-and-spoke network service such as Frame Relay typically requires the end user to designate one customer edge node to be the “hub” to which all “spoke” sites are connected. If a “spoke” site needs to communicate with another “spoke” site, the sites communicate through the “hub,” which can introduce additional transmission delay.

EMS services are “plug and play” in nature meaning that the inherent broadcast nature of Ethernet is used to discover other members connected to the EMS. As EMS is based upon Ethernet bridging techniques and is not IP based, the service is often referred to as Transparent LAN service. As many new applications use Layer 2 “heartbeat” mechanisms that cannot be routed, an EMS allows these applications to be deployed in geographically dispersed locations, which provides enhanced business continuance and availability.

It can be seen that VPLS addresses an important emerging market opportunity for service providers to offer Layer 2 multipoint VPN that connect multiple sites within a specific metropolitan geographical area. This market requirement is frequently referred to as a metropolitan-area network (MAN). The following types of services may be supported using an EMS:

- Service providers can offer geographically dispersed virtual NAP across a high-speed MPLS backbone. Using the Cisco<sup>®</sup> VPLS solution, ISPs can create a Layer 2 virtual switch over the MPLS infrastructure to create a distributed Network Access Point (NAP). This allows service providers to offer transparent private peering between multiple Internet service providers (ISPs) across an MPLS infrastructure.
- Enterprise customers have requirements to connect multiple corporate sites within a specific metro region at Layer 2. EMS services using Cisco VPLS solution enable applications that require Layer 2 connectivity between sites, such as server cluster heartbeats, to be geographically distributed, enhancing business continuity.
- Many small and midsize businesses have non-IP applications such as Microsoft Windows for Workgroups that do use NetBEUI for communications. An EMS delivered using Cisco VPLS enables these customers to interconnect multiple sites without changing their operating system configurations.
- Enterprises that desire any-to-any connectivity between sites, but do not wish to use Layer 3 VPN, may use EMS delivered via a Cisco VPLS solution.

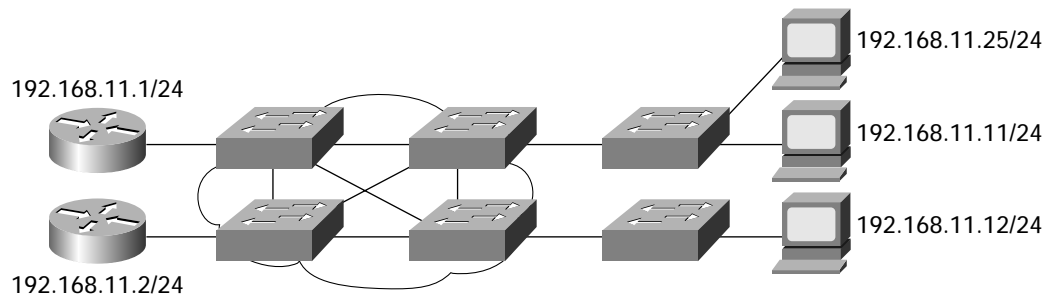
The applications that EMS may be used for vary. However, other mechanisms such as those described within the IEEE 802.1ad Provider Bridges can be used to offer EMS services using minimally modified Ethernet switches that are compatible with IETF hierarchical VPLS architectures. Cisco was the first to describe the concept of a hierarchical VPLS architecture that combined Ethernet switches with an MPLS core that provides cost-effective, feature-rich multipoint Ethernet services.



## VPLS Architecture

The VPLS architecture has been described within various IETF documents and describes how virtual Ethernet bridges (referred to as VSI) can be interconnected using MPLS pseudowires. The current VPLS working group documents describe two basic architectures—a non-hierarchical, flat architecture, as depicted in Figure 2, and a hierarchical architecture, as depicted in Figure 3.

Figure 2  
Nonhierarchical VPLS

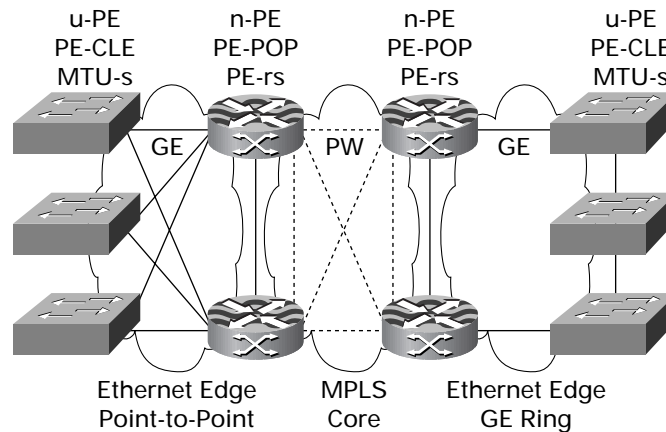


The differences between VPLS and H-VPLS are related to the scaling attributes of each solution. VPLS is a relatively simple architecture that is suitable for small-scale VPLS deployments. It requires that the edge device is MPLS-capable and it needs to participate in routing protocols and Label Distribution Protocol (LDP). This complicates the overall network operation and the edge device, which needs to hold VPLS forwarding tables, routing tables, and others. Additionally, all broadcast and multicast replication is performed at the edge device, which can decrease the efficiency of the network.

By contrast, H-VPLS partitions the network into several edge domains that are interconnected using an MPLS core. The considerations for the edge devices are now simplified, as they need only learn of their local n-PE devices and therefore do not need large routing table support. Alternatively, the edge domain can be built using Ethernet switches and techniques such as VLAN Tag Stacking, aka Q-in-Q, described within the IEEE 802.1ad Provider Bridges draft. Using Ethernet as the edge technology simplifies the operation of the edge domain and reduces the cost of the edge devices dramatically. Cisco was one of the first vendors to realize the scaling limitations imposed by having a nonhierarchical architecture, and developed the concept of a hierarchical VPLS architecture using standard Ethernet bridges at the edge and MPLS within the core.



Figure 3  
Hierarchical VPLS—Ethernet Edge and MPLS Core



The H-VPLS architecture provides an extremely flexible architectural model that enables Ethernet multipoint and point-to-point Layer 2 VPN services, as well as Ethernet access to Layer 3 VPN services, enabling service providers to offer multiple services across a single high-speed architecture.

#### Frame Forwarding

Although VPLS and Hierarchical VPLS (H-VPLS) offer differing scaling attributes, the frame forwarding mechanism is the same for both—VPLS forwards Ethernet frames using Layer 2 MAC addresses. The operation of VPLS is exactly the same as that found within IEEE 802.1 bridges in that the VSI self-learns the source MAC address to port associations and forwards frames based on the destination MAC address. If the destination address is unknown, or is a broadcast or multicast address, the frame is flooded to all ports associated with the virtual bridge.

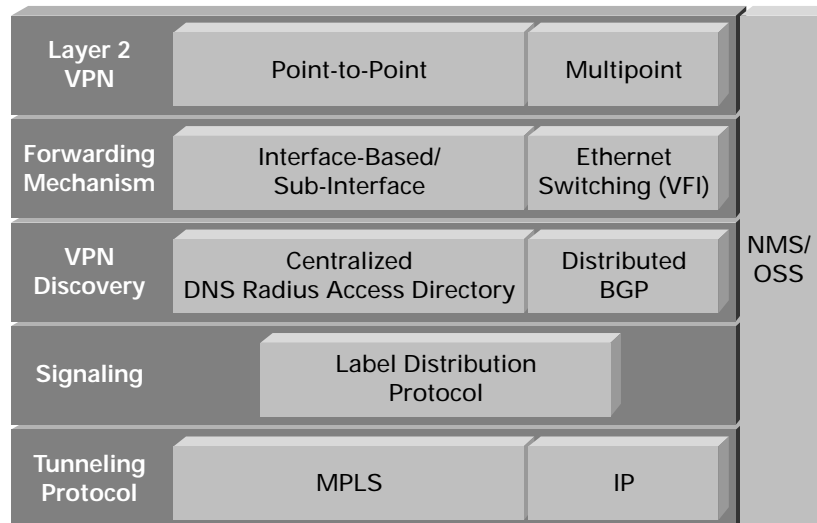
This operation is unique to Ethernet, as the Ethernet frame has a source and destination MAC address, whereas traditional WAN protocols such as Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC) lack an address field or have a destination address only (ATM and Frame Relay).

#### Auto-Discovery and Signaling

An important aspect of VPN technologies, including VPLS, is the ability of network devices to automatically discover and signal to other devices an association with a particular VPN, often referred to as discovery and signaling mechanisms. Within the context of VPLS this includes discovery of other peers associated with a particular EMS, signaling of pseudowires to link VSIs, and MAC withdrawal. Although a lot of attention is focused on these mechanisms, but it should be remembered that robust network management systems (NMS) and operational support systems (OSS) are critical elements in the deployment and management of VPNs, whether at Layer 2 or Layer 3.



Figure 4  
VPLS Discovery and Signaling Mechanisms



Discovery mechanisms can be broadly characterized as distributed mechanisms that reside within the network devices, or centralized services that the network devices query to learn VPN associations. Distributed mechanisms such as Border Gateway Protocol (BGP) and LDP require each network device to be configured with VPN associations that the discovery mechanism then advertises to other network devices. Although distributed mechanisms are desirable, they can be prone to configuration errors and to security issues such as injection of false information or denial of service (DOS) attacks. Centralized mechanisms such as Domain Name System (DNS), RADIUS, and Directory Enabled Networking (DEN) require the network devices to poll the centralized servers to learn VPN associations. These mechanisms allow more robust security to be applied and a single point of configuration, but add additional management elements to the overall network.

One additional discovery mechanism is the use of NMS/OSS that distribute VPN membership as the VPNs are created by the service management software. This provides desirable features such as service integrity and syntax checking and also provides system security as only the network devices that need to be associated with VPN are configured.

Each discovery mechanism has advantages and disadvantages that may be applicable to a particular service provider. To allow a service provider the most flexibility in choosing a discovery mechanism, the VPLS working group document, *draft-ietf-l2vpn-vpls-ldp-01.txt*, does not describe any particular discovery mechanism.

Signaling of pseudowires between provider edge devices, described in *draft-ietf-l2vpn-vpls-ldp-00*, uses targeted LDP sessions to exchange label values and attributes. As the attributes of a pseudowire connecting VSIs are point-to-point in nature (bandwidth profiles, sequence number negotiation, etc.), LDP is an efficient mechanism for signaling pseudowire status for Ethernet point-to-point and multipoint services.

## Summary

VPLS provides an architecture that provides Ethernet Multipoint Services across geographically dispersed locations using MPLS as a transport. EMSs are attractive—they offer a solution to problems that many enterprise customers and service providers are seeking to address (high-speed, secure, any-to-any forwarding at Layer 2). The requirement to forward frames at Layer 2 is important, as many new applications and services dictate that the service be transparent to upper-layer protocols (IP) or may lack network layer addressing altogether (NetBEUI).

VPLS as a standard is now a working group document within the IETF; *draft-ietf-l2vpn-vpls-ldp-01.txt* is the most widely adopted VPLS implementation, with demonstrable multivendor interoperability. A variant of VPLS, H-VPLS provides a solution to delivering Ethernet multipoint services over MPLS using either MPLS- or Ethernet-based IEEE 802.1ad provider bridges. The use of Ethernet switches at the edge offers significant technical and economic advantages compared to VPLS- or MPLS-based H-VPLS. It should be noted that H-VPLS also allows Ethernet point-to-point and multipoint Layer 2 VPN services, as well as Ethernet access to high-speed Internet and IP VPN services.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0304R) N2/KW/LW5555 01/04